

TRANSMITTAL OF APPEAL BRIEFDocket No.
66729/P032US/10614704

In re Application of: Roy Schoenberg

Application No.
10/726,423-Conf. #5827Filing Date
December 3, 2003Examiner
S. RangrejGroup Art Unit
3686

Invention: BRIDGED PATIENT/PROVIDER CENTRIC METHOD AND SYSTEM

TO THE COMMISSIONER OF PATENTS:Transmitted herewith is the Appeal Brief in this application, with respect to the Notice of Appeal filed: September 2, 2009.The fee for filing this Appeal Brief is \$ 540.00.☒ Large Entity ☐ Small Entity☐ A petition for extension of time is also enclosed.

The fee for the extension of time is _____.

☐ A check in the amount of _____ is enclosed.☐ Charge the amount of the fee to Deposit Account No. 50-3948.☒ Payment is being paid on-line by credit card.☒ The Director is hereby authorized to charge any additional fees that may be required or credit any overpayment to Deposit Account No. 50-3948.
This sheet is submitted in duplicate.

Jody C. Bishop
Attorney Reg. No. : 44,034
FULBRIGHT & JAWORSKI L.L.P.
2200 Ross Avenue, Suite 2800
Dallas, Texas 75201-2784
(214) 855-8007Dated: November 2, 2009**Appeal Brief Transmittal**

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted via the Office electronic filing system in accordance with § 1.8(a)(4).

Dated: November 2, 2009

Signature:  (Donna Forbit)

Appeal Brief

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted via the Office electronic filing system in accordance with § 1.6(a)(4).

Dated November 2, 2009

Signature

Donna Forbit
(Donna Forbit)

Docket No.: 66729/P032US/10614704
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Roy Schoenberg

Application No.: 10/726,423

Confirmation No.: 5827

Filed: December 3, 2003

Art Unit: 3686

For: BRIDGED PATIENT/PROVIDER CENTRIC
METHOD AND SYSTEM

Examiner: S. Rangrej

APPEAL BRIEF

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

As required under 37 C.F.R. § 41.37(a), this brief is filed within two months of the Notice of Appeal filed September 2, 2009, and is in furtherance of said Notice of Appeal.

The fees required under 37 C.F.R. § 41.20(b)(2) are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains items under the following headings as required by 37 C.F.R. § 41.37 and M.P.E.P. § 1206:

- I. Real Party In Interest
- II. Related Appeals and Interferences
- III. Status of Claims
- IV. Status of Amendments
- V. Summary of Claimed Subject Matter
- VI. Grounds of Rejection to be Reviewed on Appeal
- VII. Argument
- VIII. Claims Appendix
- IX. Evidence Appendix
- X. Related Proceedings Appendix

I. REAL PARTY IN INTEREST

The real party in interest for this appeal is:

The TriZetto Group, Inc.

II. RELATED APPEALS, INTERFERENCES, AND JUDICIAL PROCEEDINGS

There are no other appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS

A. Total Number of Claims in Application

There are 39 claims pending in application, numbered 1-5 and 7-40.

B. Current Status of Claims

1. Claims canceled: None
2. Claims withdrawn from consideration but not canceled: None
3. Claims pending: 1-5 and 7-40
4. Claims allowed: None
5. Claims rejected: 1-5 and 7-40

C. Claims On Appeal

The claims on appeal are claims 1-5 and 7-40.

IV. STATUS OF AMENDMENTS

A Final Office Action was mailed August 14, 2009, which finally rejected claims 1-5 and 7-40. In response, Applicant filed a notice of appeal with an accompanying Pre-Appeal Brief Request for Review (on September 2, 2009). A Notice of Panel Decision was mailed September 22, 2009, which indicated that at least one issue remains for appeal.

Accordingly, this brief is submitted in support of the notice of appeal filed September 2, 2009. Because no claim amendments have been presented after the Final Office Action of August 14, 2009, the claims on appeal are those as rejected in that Final Office Action. A complete listing of the claims is provided in the Claims Appendix hereto.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The following provides a concise explanation of the subject matter defined in each of the separately argued claims involved in the appeal, referring to the specification by page and line number and to the drawings by reference characters, as required by 37 C.F.R. § 41.37(c)(1)(v). Each element of the claims is identified by a corresponding reference to the specification and drawings where applicable. It should be noted that the citation to passages in the specification and drawings for each claim element does not imply that the limitations from the specification and drawings should be read into the corresponding claim element.

According to one claimed embodiment, such as that of independent claim 1, a key organization method is provided. The method comprises receiving (e.g., operational block 120 of FIGURE 4), by a key organization system operable on a computer processor (e.g., key organization system 10 of FIGURES 1-2), a first access key (e.g., access key 12 of FIGURES 1-2) that grants, to a medical service provider (e.g., medical service provider 18 of FIGURE 1), a patient-defined level of access to a first set of medical records (e.g., set of medical records 60 shown in FIGURE 2), *see e.g.*, paragraph 0030 at lines 8-16 on page 8 of the application. The method further comprises receiving, by said key organization system, a second access key (e.g., access key 14 of FIGURES 1-2) that grants, to said medical service provider, a patient-defined level of access to a second set of medical records (e.g., set of medical records 62 in FIGURE 2), *see e.g.*, paragraph 0030 at lines 8-16 on page 8 of the application. The method further comprises storing the first and second access keys in a centralized key repository that is communicatively accessible by said key organization system (e.g., key repository 50 of FIGURE 2), and associating (e.g., operational block 122 of FIGURE 4), by said key organization system, said first and second access keys with said medical service provider, *see e.g.*, paragraph 0030 at lines 8-16 on page 8 of the application.

In certain embodiments, such as that of dependent claim 4, the method further comprises controlling, by said key organization system, said medical service provider's access to the first set of medical records by allowing said medical service provider to select, from a list of patients for whom access keys are associated with said medical service provider (e.g., the list 160 of

patients in FIGURE 6), a corresponding patient to whom the first set of medical records pertains, *see e.g.*, paragraphs 0031-0041 at page 8, line 17 – page 11, line 5 of the application.

In certain embodiments, such as that of dependent claim 5, the method further comprises controlling, by said key organization system, said medical service provider's access to the second set of medical records by allowing said medical service provider to select, from said list of patients (e.g., list 160 of patients in FIGURE 6), a corresponding patient to whom the second set of medical records pertains, *see e.g.*, paragraphs 0031-0041 at page 8, line 17 – page 11, line 5 of the application.

According to one embodiment, such as that of dependent claim 37, the method further comprises granting said medical service provider secure access to said key organization system, wherein said access allows said medical service provider to select a patient from a group of patients associated with said medical service provider, *see e.g.*, paragraph 0034 at page 9, lines 11-15 of the application.

According to one embodiment, such as that of dependent Claim 38, the secure access is granted after said medical service provider passes a security test issued by said key organization system, *see e.g.*, paragraph 0034 at page 9, lines 11-15 of the application (the medical service provider logs into the key organization system).

According to one embodiment, such as that of dependent claim 39, the method further comprises receiving, by said key organization system, said selection (of a patient from the list of patients for whom an access key is associated with the medical service provider), wherein said selection is a request to access said first set of medical records; retrieving from said centralized key repository, by said key organization system in response to said selection, said first access key; and using, by said key organization system, said first access key to control said medical services provider's access to said first set of medical records, *see e.g.*, paragraphs 0031-0041 at page 8, line 17 – page 11, line 5 of the application.

According to another claimed embodiment, such as that of independent claim 12, a key distribution method comprises receiving (e.g., operational block 120 of FIGURE 4), by the key organization system (e.g., key organization system 10 of FIGURES 1-2) from a first patient (e.g., patient 20 of FIGURE 1) using a client computer (e.g., client computer 32 of FIGURE 1), a first access key (e.g., access key 12 of FIGURES 1-2) that grants, to a medical service provider (e.g., medical service provider 18 of FIGURE 1), a patient-defined level of access to a first set of medical records (e.g., set of medical records 60 shown in FIGURE 2), *see e.g.*, paragraph 0030 at lines 8-16 on page 8 of the application. The method further comprises receiving, by the key organization system from a second patient (e.g., patient 22 of FIGURE 1) using a second client computer (e.g., the client computer shown in FIGURE 1 as associated with patient 22), a second access key (e.g., access key 14 of FIGURES 1-2) that grants, to said medical service provider, a patient-defined level of access to a second set of medical records (e.g., set of medical records 62 of FIGURE 2), *see e.g.*, paragraph 0030 at lines 8-16 on page 8 of the application. The method further comprises associating (e.g., operational block 122 of FIGURE 4), by said key organization system, said first and second access keys to said medical service provider, and storing, by said key organization system, the first and second access keys and said association in a centralized key repository (e.g., centralized key repository 50 of FIGURE 2), *see e.g.*, paragraph 0030 at lines 8-16 on page 8 of the application. The method further comprises receiving, by said key organization system, a request from said medical service provider to access said first or second set of medical records and, responsive to said request, controlling access to said requested set of medical records using said first or second access key, wherein input of said first or second access key from said medical service provider is not required by said key organization system, *see e.g.*, paragraphs 0031-0041 at page 8, line 17 – page 11, line 5 of the application.

According to one embodiment, such as that of dependent claim 13, the method further comprises controlling, by said key organization system, said medical service provider's access to the first set of medical records by receiving input from said medical service provider for selecting, from a list of patients (e.g., list 160 of FIGURE 6) for whom access keys are associated with said medical service provider, a corresponding patient to whom the first set of

medical records pertains, *see e.g.*, paragraphs 0031-0041 at page 8, line 17 – page 11, line 5 of the application.

According to one embodiment, such as that of dependent claim 14, the method further comprises controlling, by said key organization system, said medical service provider's access to the second set of medical records by receiving input from said medical service provider for selecting, from a list of patients (e.g., list 160 of FIGURE 6) for whom access keys are associated with said medical service provider, a corresponding patient to whom the second set of medical records pertains, *see e.g.*, paragraphs 0031-0041 at page 8, line 17 – page 11, line 5 of the application.

According to another claimed embodiment, such as that of independent claim 19, a key organization method comprises maintaining, on a remote server (e.g., server 26 of FIGURE 1), a centralized key repository (e.g., centralized key repository 50 of FIGURE 2) and a centralized medical record repository (e.g., centralized medical record repository 52 of FIGURE 2), *see e.g.*, paragraphs 0030-0031 at lines 8-21 on page 8 of the application.. The method further comprises storing a plurality of patient medical records (e.g., medical records 60-64 of FIGURE 2) on the centralized medical record repository, wherein said plurality of patient medical records comprise at least of a first set of medical records (e.g., set 60 of medical records in FIGURE 2) containing medical information pertaining a first patient (e.g., patient 20 of FIGURE 1) and a second set of medical records (e.g., set 62 of medical records in FIGURE 2) containing medical information pertaining a second patient (e.g., patient 22 of FIGURE 1), *see e.g.*, paragraph 0024 at page 6, line 18 – page 7, line 2 of the application. The method further comprises storing, in said centralized key repository, a plurality of access keys (e.g., keys 12-16 of FIGURES 1-2) that each grant patient-defined access rights to a corresponding patient's set of medical records, *see e.g.*, paragraph 0030 at lines 8-16 on page 8 of the application. The method further comprises, responsive to a request received from a medical service provider to access one of said sets of medical records, retrieving, by a key organization system (e.g., key organization system 10 of FIGURES 1-2), from said centralized key repository a determined one of said access keys that is associated with said medical service provider (e.g., operational block 122 of FIGURE 4) and

which corresponds to said requested set of medical records, and controlling, by said key organization system, access by said medical service provider to said requested set of medical records using the retrieved access key, *see e.g.*, paragraphs 0031-0041 at page 8, line 17 – page 11, line 5 of the application.

According to one embodiment, such as that of dependent claim 21, the method further comprises storing, by said key organization system, the first and second access keys in the centralized key repository, *see e.g.*, paragraph 0030 at lines 8-16 on page 8 of the application.

According to one embodiment, such as that of dependent claim 22, the method further comprises accessing, by said key organization system, the first set of medical records using the first access key, *see e.g.*, paragraph 0036 at page 9, line 25 – page 10, line 7 of the application.

According to one embodiment, such as that of dependent claim 23, the method further comprises accessing, by said key organization system, the second set of medical records using the second access key, *see e.g.*, paragraph 0036 at page 9, line 25 – page 10, line 7 of the application.

According to another claimed embodiment, such as that of independent claim 28, a key organization system (e.g., key organization system 10 of FIGURES 1-2) comprises a server system (e.g., server 26 of FIGURE 1) including a computer processor and associated memory, the server system having a centralized key repository (e.g., centralized key repository 50 of FIGURE 2) and a centralized medical record repository (e.g., centralized medical record repository 52 of FIGURE 2). The server system is configured to: store a first set of medical records (e.g., set 60 of medical records in FIGURE 2) and a second set of medical records (e.g., set 62 of medical records in FIGURE 2) on the centralized medical record repository (*see e.g.*, paragraph 0024 at page 6, line 18 – page 7, line 2 of the application); receive a first access key (e.g., access key 12 of FIGURES 1-2) associated with a medical service provider (e.g., operational block 122 of FIGURE 4) that grants to said medical service provider a patient-defined level of access to the first set of medical records (*see e.g.*, paragraph 0030 at lines 8-16 on page 8 of the application); receive a second access key (e.g., access key 14 of FIGURES 1-2)

associated with said medical service provider that grants to said medical service provider a patient-defined level of access to the second set of medical records (*see e.g.*, paragraph 0030 at lines 8-16 on page 8 of the application); and store the first access key and the second access key on the centralized key repository, *see e.g.*, paragraph 0030 at lines 8-16 on page 8 of the application. The key organization system is configured to, responsive to receipt of a request from the medical service provider to access one of said first and second set of medical records, retrieve a determined one of the first and second access keys from the centralized key repository and use the retrieved access key to control access by said medical service provider to said requested set of medical records, *see e.g.*, paragraphs 0031-0041 at page 8, line 17 – page 11, line 5 of the application.

According to another claimed embodiment, such as that of independent claim 34, a computer program product residing on a computer readable medium having a plurality of instructions stored thereon which, when executed by the processor, cause a key organization system (e.g., key organization system 10 of FIGURES 1-2) to: receive, at said key organization system, a first access key (e.g., access key 12 of FIGURES 1-2) that grants to a first medical service provider a first patient-defined level of access to a first set of medical records (e.g., set 60 of medical records in FIGURE 2) of a corresponding patient (*see e.g.*, paragraph 0030 at lines 8-16 on page 8 of the application); receive, at said key organization system, a second access key (e.g., access key 14 of FIGURES 1-2) that grants to a second medical service provider a second patient-defined level of access to said first set of medical records of said corresponding patient (*see e.g.*, paragraphs 0030-0033 at page 8, line 8 – page 9, line 10 of the application); store the first and second access keys in a centralized key repository (e.g., centralized key repository 50 of FIGURE 2); and responsive to a request received from one of said first and second medical service providers to access said first set of medical records, retrieve from said centralized key repository a determined one of said access keys that is associated with said requesting medical service provider, and using the retrieved access key to grant to the requesting medical service provider the corresponding patient-defined level of access to said first set of medical records, *see e.g.*, paragraphs 0031-0041 at page 8, line 17 – page 11, line 5 of the application.

According to another claimed embodiment, such as that of independent claim 35, a computer program product residing on a computer readable medium having a plurality of instructions stored thereon which, when executed by the processor, cause a key organization system (e.g., key organization system 10 of FIGURES 1-2) to: receive, from a patient (e.g., patient 20 of FIGURE 1) at a key organization system, a first access key (e.g., access key 12 of FIGURES 1-2) associated with a first medical service provider (e.g., operational block 122 of FIGURE 4) that grants to said first medical service provider a first patient-defined level of access to a first set of medical records (e.g., set 60 of medical records in FIGURE 2, and *see e.g.*, paragraph 0030 at lines 8-16 on page 8 of the application); receive, from said patient at said key organization system, a second access key (e.g., access key 14 of FIGURES 1-2) associated with a second medical service provider that grants to said second medical service provider a second patient-defined level of access to said first set of medical records (*see e.g.*, paragraphs 0030-0033 at page 8, line 8 – page 9, line 10 of the application); store the first and second access keys in a centralized key repository (e.g., centralized key repository 50 of FIGURE 2); receive a request from said first medical service provider to access said first set of medical records (*see e.g.*, paragraphs 0031-0041 at page 8, line 17 – page 11, line 5 of the application); and retrieve, responsive to said request, said first access key from said centralized key repository to provide said first medical service provider with access to said first set of medical records wherein input of said first access key from said first medical service provider is not required by said key organization system, *see e.g.*, paragraphs 0031-0041 at page 8, line 17 – page 11, line 5 of the application.

According to another claimed embodiment, such as that of independent claim 36, a computer program product residing on a computer readable medium that is communicatively coupled to a server (e.g., server 26 of FIGURE 1) having a plurality of instructions stored thereon which, when executed by a processor of the server cause a key organization system (e.g., key organization system 10 of FIGURES 1-2) to: store (operational block 140 of FIGURE 5) a plurality of patient-associated medical records (e.g., medical records 60-64 of FIGURE 2) on a centralized medical record repository (e.g., centralized medical record repository 52 of FIGURE 2), wherein said plurality of patient-associated medical records comprise at least of a first set

(e.g., set 60 of FIGURE 2) of medical records associated with a first patient (e.g., patient 20 of FIGURE 1) and a second set (e.g., set 62 of FIGURE 2) of medical records associated with a second patient (e.g., patient 22 of FIGURE 1), *see e.g.*, paragraph 0024 at page 6, line 18 – page 7, line 2 of the application; store a plurality of provider-associated (e.g., operational block 122 of FIGURE 4) access keys (e.g., access keys 12-16 of FIGURES 1-2) on a centralized key repository (e.g., centralized key repository 50 of FIGURE 2), wherein said plurality of provider-associated access keys comprise a first access key (e.g., access key 12 of FIGURES 1-2) that grants a patient-defined level of access to the first set of medical records and a second access key (e.g., access key 14 of FIGURES 1-2) that grants a patient-defined level of access to the second set of medical records (*see e.g.*, paragraphs 0030-0033 at page 8, line 8 – page 9, line 10 of the application); responsive to a received request from a provider to access one of said first and second sets of medical records, retrieve from said centralized key repository a respective one of said first and second access keys that grants the requesting provider a patient-defined level of access to the requested one of said first and second sets of medical records (*see e.g.*, paragraphs 0031-0041 at page 8, line 17 – page 11, line 5 of the application); and use said retrieved access key to grant said requesting provider the corresponding patient-defined level of access to the requested one of said first and second sets of medical records (*see e.g.*, paragraphs 0031-0041 at page 8, line 17 – page 11, line 5 of the application).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. Claims 1-5 and 7-40 are rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,941,271 to Soong (hereinafter “*Soong*”).

VII. ARGUMENT

Appellant respectfully traverses the outstanding rejections of the pending claims, and requests that the Board reverse the outstanding rejections in light of the remarks contained herein. The claims do not stand or fall together. Instead, Appellant presents separate arguments for various independent and dependent claims. Each of these arguments is separately argued below and presented with separate headings and sub-heading as required by 37 C.F.R. § 41.37(c)(1)(vii).

A. Rejection of Claims Under 35 U.S.C. §102 Over *Soong*

Claims 1-36 stand rejected under 35 U.S.C. § 102(e) as being anticipated by *Soong*. However, it is well settled that to anticipate a claim, a reference must teach every element of the claim, see M.P.E.P. § 2131. Moreover, in order for a reference to be anticipatory under 35 U.S.C. § 102 with respect to a claim, “[t]he elements must be arranged as required by the claim,” see M.P.E.P. § 2131, citing *In re Bond*, 15 U.S.P.Q.2d 1566 (Fed. Cir. 1990). Furthermore, in order for a reference to be anticipatory under 35 U.S.C. § 102 with respect to a claim, “[t]he identical invention must be shown in as complete detail as is contained in the . . . claim,” see M.P.E.P. § 2131, citing *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 U.S.P.Q.2d 1913, 1920 (Fed. Cir. 1989). Appellant respectfully asserts that the rejections do not satisfy these requirements, as detailed below.

Brief Discussion of *Soong*

Before addressing the individual claims, Appellant first discusses the applied *Soong* reference for the convenience of the Board.

Soong generally discloses a traditional patient-centric method used for managing access to centrally-stored medical records in a web accessible database. In *Soong*'s traditional system, patient medical records are stored in a centralized database (*Soong* at col. 5, lns. 4-6) which allows a patient to create a password granting to access those files. *Soong* at col. 6, lns. 50-53. Once the patient is given a password, the patient can distribute the password to other individuals, such as physicians, who can use that password to log into the *Soong*'s system and access the records. *Soong* at col. 6, lns. 50-53. For example, if a patient wants his podiatrist, cardiologist, and physiatrist to have access to his medical records, the patient gives each of his doctors the password. *See Soong* at col. 6, lns. 50-53.

Once a doctor has a patient's password, when accessing the patient's medical records, the doctor must log into *Soong*'s system and input the patient's password. *Soong* at col. 6, lns. 19-25. Once the password is entered, the *Soong*'s system verifies the password and allows access if the password is valid. *Soong* at col. 6, lns. 28-32.

In *Soong*, the doctor is required to maintain the patient's password after receiving it from the patient, and the doctor is required to directly input the patient's password when requesting to access the patient's medical records. Thus, the burden is placed on the individual physicians to maintain and input the various passwords provided the physicians by their patients. This typically leads to considerable overhead for the physicians because each physician must maintain a long list of passwords due to the multitude of patients providing individual passwords. *Soong* does not propose any intermediary key organization system to aid in managing the various patient-defined access keys for facilitating access by the medical service providers to the patient's medical records.

Further, *Soong* does not associate the passwords with any medical service provider (e.g., doctor) to whom the corresponding access rights are granted. Instead, *Soong* associates a password with corresponding access rights, and then the site computer grants those access rights to any user who inputs the password. Thus, any user possessing the password can directly input that password to gain the corresponding access rights to the patient's medical records.

Independent Claim 1 and Dependent Claims 2-3 and 7-11

Independent claim 1 recites:

A key organization method comprising:

receiving, by a key organization system operable on a computer processor, a first access key that grants, to a medical service provider, a patient-defined level of access to a first set of medical records;

receiving, by said key organization system, a second access key that grants, to said medical service provider, a patient-defined level of access to a second set of medical records;

storing the first and second access keys in a centralized key repository that is communicatively accessible by said key organization system; and

associating, by said key organization system, said first and second access keys with said medical service provider. (Emphasis added).

Soong fails to teach at least the above-emphasized limitations of claim 1, as discussed below.

Receiving and Storing Access Keys

The *Office Action* likens *Soong*'s password to the claimed "access keys." *Office Action* at 2. However, *Soong* does not teach a key organization system that receives and stores access keys. *Soong*'s distribution of passwords does not teach the limitation. Specifically, *Soong* teaches that the patient can provide the password to others. *Soong* at col. 6, Ins. 50-54. However, in *Soong*, the distributed passwords are not taught as stored in any intermediary system (e.g. a key organization system). Rather, after the passwords are distributed in *Soong*, it becomes the responsibility of the individual recipients of such passwords (e.g., the medical providers) to keep track of the passwords and to input the passwords when accessing the medical records. *Soong* at col. 6, Ins. 49-59. As such, *Soong* does not teach a key organization system receiving

and storing access keys that grant a medical service provider a patient-defined level of access to medical records, as recited by claim 1.

Therefore the rejection of claim 1 should be overturned for at least this reason.

Associating Access Keys

In addition, *Soong* fails to teach “associating, by said key organization system, said first and second access keys with said medical service provider”. *Soong*’s passwords are not associated with a medical provider. In *Soong*, the patient merely provides his password to whomever (e.g. family members, friends, health care professionals), and any of those individuals use that same patient password to access the medical records. *Soong* at col. 6, lns. 5-6, 50-54. Thus, *Soong* fails to disclose a key organization system that associates access keys with a medical service provider.

While the password discussed in *Soong* may define certain access rights that are presumed by the system as being granted to the individual inputting the password, *Soong*’s system does not associate the password with any medical service provider. For instance, the system in *Soong* makes no determination of whether a given password has been granted to a particular medical service provider (or other user) who is requesting access to the medical records, but instead merely requires the requestor to input the password.

Therefore, claim 1 is not anticipated by *Soong*, and thus the rejection of claim 1 should be overturned for the above reasons. Dependent claims 2-3 and 7-11 each depend either directly or indirectly from independent claim 1 and are thus believed to likewise be allowable over the applied reference based at least on their dependency from claim 1 for the reasons discussed above.

Dependent Claims 4 and 40

Dependent claim 4 depends from independent claim 1 and thus inherits all limitations of claim 1. Therefore, dependent claim 4 is believed allowable over the applied reference based at least on its dependency from claim 1 for the reasons presented above.

Dependent claim 4 further recites “controlling, by said key organization system, said medical service provider’s access to the first set of medical records by allowing said medical

service provider to select, from a list of patients for whom access keys are associated with said medical service provider, a corresponding patient to whom the first set of medical records pertains” (emphasis added). *Soong* fails to teach at least the above-emphasized limitation of dependent claim 4. *Soong* does not teach that its access keys are associated with a medical service provider, and thus it does not teach that a key organization system allows a medical service provider to select, from a list of patients for whom access keys are associated with the medical service provider, a corresponding patient to whom the first set of medical records pertains, as recited by claim 4. *Soong* does not disclose any such selection from a list, but instead merely provides that for a given patient a physician may directly input that patient’s password in order to access the given patient’s medical records.

Thus, claim 4 is not anticipated by *Soong*, and therefore the rejection of claim 4 should be overturned for this further reason. Further, claim 40 depends from claim 4 and is thus likewise believed to be allowable based at least on its dependency from claim 4 for the reasons discussed above and with independent claim 1.

Dependent Claim 5

Dependent claim 5 depends from claim 4 which depends from independent claim 1, and thus claim 4 inherits all limitations of claims 1 and 4. Therefore, dependent claim 5 is believed allowable over the applied reference based at least on its dependency from claims 1 and 4 for the reasons presented above.

Dependent claim 5 further recites “controlling, by said key organization system, said medical service provider’s access to the second set of medical records by allowing said medical service provider to select, from said list of patients, a corresponding patient to whom the second set of medical records pertains” (emphasis added). *Soong* fails to teach at least the above-emphasized limitation of dependent claim 5. Again, as discussed above with claim 4, *Soong* does not teach that its access keys are associated with a medical service provider, and thus it does not teach that a key organization system allows a medical service provider to select, from a list of patients for whom access keys are associated with the medical service provider, a corresponding patient to whom a second set of medical records pertains, as recited by claim 5.

Thus, claim 5 is not anticipated by *Soong*, and therefore the rejection of claim 5 should be overturned for this further reason.

Dependent Claim 37

Dependent claim 37 depends from independent claim 1 and thus inherits all limitations of claim 1. Therefore, dependent claim 37 is believed allowable over the applied reference based at least on its dependency from claim 1 for the reasons presented above.

Dependent claim 37 further recites “granting said medical service provider secure access to said key organization system, wherein said access allows said medical service provider to select a patient from a group of patients associated with said medical service provider” (emphasis added). *Soong* fails to teach at least the above-emphasized limitation of dependent claim 37. *Soong* does not teach a key organization system to which a medical service provider gains secure access and then allows the medical service provider to select a patient from a group of patients associated with the medical service provider. Instead, in *Soong* a medical service provider directly inputs a password (received from a patient) in order to gain access to that patient’s medical records.

Thus, claim 37 is not anticipated by *Soong*, and therefore the rejection of claim 37 should be overturned for this further reason.

Dependent Claim 38

Dependent claim 38 depends from claim 37 which depends from independent claim 1, and thus dependent claim 38 inherits all limitations of claims 1 and 37. Therefore, dependent claim 38 is believed allowable over the applied reference based at least on its dependency from claims 1 and 37 for the reasons presented above.

Dependent claim 38 further recites “wherein said secure access is granted after said medical service provider passes a security test issued by said key organization system.” *Soong* fails to teach this further limitation of claim 38. There is no security test issued by a key organization system in order for a medical service provider to gain secure access to such a key

organization system in *Soong*. Instead, in *Soong* a medical service provider directly inputs a password (received from a patient) in order to gain access to that patient's medical records.

Thus, claim 38 is not anticipated by *Soong*, and therefore the rejection of claim 38 should be overturned for this further reason.

Dependent Claim 39

Dependent claim 39 depends from claim 37 which depends from independent claim 1, and thus dependent claim 39 inherits all limitations of claims 1 and 37. Therefore, dependent claim 39 is believed allowable over the applied reference based at least on its dependency from claims 1 and 37 for the reasons presented above.

Dependent claim 39 further recites:

receiving, by said key organization system, said selection, wherein said selection is a request to access said first set of medical records;
retrieving from said centralized key repository, by said key organization system in response to said selection, said first access key; and
using, by said key organization system, said first access key to control said medical services provider's access to said first set of medical records.

Soong fails teach these further limitations of claim 39. First, *Soong* does not teach a key organization system that retrieves, in response to a selection of a patient from a list of patients, an access key from a centralized key repository. Instead, *Soong* proposes a system in which a medical service provider directly inputs a password that is specific for a given patient when accessing the given patient's medical records. Further, *Soong* does not teach a key organization system that uses an access key that is retrieved from a centralized key repository to control the access of the requesting medical service provider to the medical records.

Thus, claim 39 is not anticipated by *Soong*, and therefore the rejection of claim 39 should be overturned for this further reason.

Independent Claim 12 and Dependent Claims 15-18

Independent claim 12 recites:

A key distribution method comprising:
receiving, by the key organization system from a first patient using a client computer, a first access key that grants, to a medical service provider, a patient-defined level of access to a first set of medical records;
receiving, by the key organization system from a second patient using a second client computer, a second access key that grants, to said medical service provider, a patient-defined level of access to a second set of medical records; and
associating, by said key organization system, said first and second access keys to said medical service provider;
storing, by said key organization system, the first and second access keys and said association in a centralized key repository; and
receiving, by said key organization system, a request from said medical service provider to access said first or second set of medical records and, responsive to said request, controlling access to said requested set of medical records using said first or second access key, wherein input of said first or second access key from said medical service provider is not required by said key organization system. (Emphasis added).

Soong fails to teach at least the above-emphasized limitations of claim 12, as discussed below.

Receiving and Storing Access Keys

As discussed above with independent claim 1, the *Office Action* likens *Soong*'s password to the claimed "access keys." *Office Action* at 2. However, *Soong* does not teach a key organization system that receives and stores access keys. *Soong*'s distribution of passwords does not teach the limitation. Specifically, *Soong* teaches that the patient can provide the password to others. *Soong* at col. 6, lns. 50-54. However, in *Soong*, the distributed passwords are not taught as stored in any intermediary system (e.g. a key organization system). Rather, after the passwords are distributed in *Soong*, it becomes the responsibility of the individual recipients of such passwords (e.g., the medical providers) to keep track of the passwords and to input the passwords when accessing the medical records. *Soong* at col. 6, lns. 49-59. As such, *Soong* does

not teach a key organization system receiving and storing access keys that grant a medical service provider a patient-defined level of access to medical records, as recited by claim 12.

Therefore the rejection of claim 12 should be overturned for at least this reason.

Associating Access Keys

In addition, *Soong* fails to teach ““associating, by said key organization system, said first and second access keys to said medical service provider ... storing, by said key organization system, the first and second access keys and said association in a centralized key repository”, as recited by claim 12. *Soong*’s passwords are not associated with a medical provider, nor is any such association stored in a centralized key repository. Rather, in *Soong*, the patient merely provides his password to whomever (e.g. family members, friends, health care professionals), and any of those individuals use that same patient password to access the medical records. *Soong* at col. 6, lns. 5-6, 50-54. Thus, *Soong* fails to disclose a key organization system that associates access keys with a medical service provider, nor is any such association stored in a centralized key repository in *Soong*.

While the password discussed in *Soong* may define certain access rights that are presumed by the system as being granted to the individual inputting the password, *Soong*’s system does not associate the password with any medical service provider. For instance, the system in *Soong* makes no determination of whether a given password has been granted to a particular medical service provider (or other user) who is requesting access to the medical records, but instead merely requires the requestor to input the password.

Therefore the rejection of claim 12 should be overturned for this further reason.

Provider Accesses Medical Records without Inputting the Access Key

In addition, *Soong* fails to teach “receiving, by said key organization system, a request from said medical service provider to access said first or second set of medical records and, responsive to said request, controlling access to said requested set of medical records using said first or second access key, wherein input of said first or second access key from said medical

service provider is not required by said key organization system" (emphasis added), as recited by claim 12.

Soong does not allow a service provider to access medical records without first inputting a password received from the patient (which the Office Action equates to the recited "access keys"). *Soong* at col. 6, lns. 20-25. Rather, *Soong* requires that the patient's password be entered by the individual person requesting the medical records before access to the records will be provided. *Soong* at col. 6, lns. 20-25.

On the other hand, in certain embodiments of the present invention, the key organization system uses the access keys for controlling access by a medical service provider to the medical records without requiring the medical service provider to maintain and input the access keys. Thus, whereas *Soong* requires a provider to input a password to the site computer in order to access the medical records of a particular patient who supplied the password to the provider, in certain embodiments of the present invention, the key organization system does not put the burden of maintaining and inputting to the key organization system different access keys for different patients in order to gain the patient-defined level of access to the patient medical records.

As a simple example, if an access key or password of "access_1" is used in *Soong* for controlling access to a given patient's medical records, the patient would send that password to his medical service provider and the medical service provider would then enter that password when accessing the patient's medical records. However, in accordance with one embodiment of the present invention, such access key of "access_1" may instead be stored to a key organization system and associated with the patient's medical service provider, and then the patient's medical service provider may access the key organization system (e.g., with a separate login that is specific to that medical service provider) and the key organization system then uses the "access_1" access key to allow the medical service provider the corresponding access rights to the patient's medical records without requiring the medical service provider to input (or even be aware of) the "access_1" access key.

As such, *Soong* does not teach this further limitation of claim 12, and thus the rejection of this claim should be overturned for this further reason. Dependent claims 15-18 each depend either directly or indirectly from independent claim 12 and are thus believed to likewise be allowable over the applied reference based at least on their dependency from claim 12 for the reasons discussed above.

Dependent Claim 13

Dependent claim 13 depends from independent claim 12 and thus inherits all limitations of claim 12. Therefore, dependent claim 13 is believed allowable over the applied reference based at least on its dependency from claim 12 for the reasons presented above.

Dependent claim 13 further recites “controlling, by said key organization system, said medical service provider’s access to the first set of medical records by receiving input from said medical service provider for selecting, from a list of patients for whom access keys are associated with said medical service provider, a corresponding patient to whom the first set of medical records pertains” (emphasis added). *Soong* fails to teach at least the above-emphasized limitation of dependent claim 13. *Soong* does not teach that its access keys (passwords) are associated with a medical service provider, and thus it does not teach that a key organization system receives input from a medical service provider for selecting, from a list of patients for whom access keys are associated with the medical service provider, a corresponding patient to whom the first set of medical records pertains, as recited by claim 13. *Soong* does not disclose any such selection from a list, but instead merely provides that for a given patient a physician may directly input that patient’s password in order to access the given patient’s medical records.

Thus, claim 13 is not anticipated by *Soong*, and therefore the rejection of claim 13 should be overturned for this further reason.

Dependent Claim 14

Dependent claim 14 depends from independent claim 12 and thus inherits all limitations of claim 12. Therefore, dependent claim 14 is believed allowable over the applied reference based at least on its dependency from claim 12 for the reasons presented above.

Dependent claim 14 further recites “controlling, by said key organization system, said medical service provider’s access to the second set of medical records by receiving input from said medical service provider for selecting, from a list of patients for whom access keys are associated with said medical service provider, a corresponding patient to whom the second set of medical records pertains” (emphasis added). *Soong* fails to teach at least the above-emphasized limitation of dependent claim 14. *Soong* does not teach that its access keys (passwords) are associated with a medical service provider, and thus it does not teach that a key organization system receives input from a medical service provider for selecting, from a list of patients for whom access keys are associated with the medical service provider, a corresponding patient to whom the second set of medical records pertains, as recited by claim 14. *Soong* does not disclose any such selection from a list, but instead merely provides that for a given patient a physician may directly input that patient’s password in order to access the given patient’s medical records.

Thus, claim 14 is not anticipated by *Soong*, and therefore the rejection of claim 14 should be overturned for this further reason.

Independent Claim 19 and Dependent Claims 20 and 24-27

Independent claim 19 recites:

A key organization method comprising:
maintaining, on a remote server, a centralized key repository and a centralized medical record repository;
storing a plurality of patient medical records on the centralized medical record repository, wherein said plurality of patient medical records comprise at least of a first set of medical records containing medical information pertaining a first patient and a second set of medical records containing medical information pertaining a second patient;
storing, in said centralized key repository, a plurality of access keys that each grant patient-defined access rights to a corresponding patient's set of medical records; and
responsive to a request received from a medical service provider to access one of said sets of medical records, retrieving, by a key organization system, from said centralized key repository a determined one of said access keys that is associated with said medical service provider and which corresponds to said requested set of medical records, and controlling, by said key organization system, access by said medical service provider to said requested set of medical records using the retrieved access key. (Emphasis added).

Soong fails to teach at least the above-emphasized limitation of claim 19. Rather than retrieving and using a key from a centralized key repository, *Soong* requires a requesting user (e.g., physician) to input a password that is used for controlling access to the medical records.

Soong does not teach a key organization system that, responsive to a request received from a medical service provider to access a set of medical records, retrieves a from a centralized key repository a determined one of the access keys that is associated with said medical service provider and which corresponds to said requested set of medical records. As discussed above with independent claims 1 and 12, *Soong* does not disclose any association of access keys with medical service providers. In *Soong*, the password for a patient's medical records may be distributed by the patient to any other user (e.g., physician, family member, etc.), and any user possessing the password is able to access the patient's medical records. The password in *Soong* is not associated with any medical service provider in any manner that enables a key organization system to determine an access key that is associated with a medical service provider

who is requesting access to the patient's medical records. Thus, *Soong* fails to teach this limitation of claim 19.

Further, *Soong* does not teach a key organization system that controls access by the medical service provider to the requested set of medical records using the access key retrieved by the key organization system. Instead, *Soong* requires a requesting user (e.g., physician) to input a password that is used for controlling access to the medical records. No key organization system is proposed by *Soong* for retrieving an access key that is associated with a medical service provider and using that retrieved access key for controlling access to medical records.

Accordingly, *Soong* fails to teach all limitations of claim 19, and thus fails to anticipate claim 19 under 35 U.S.C. §102. Therefore, the rejection of claim 19 should be overturned for the above reasons. Dependent claims 20 and 24-27 each depend either directly or indirectly from independent claim 19 and are thus believed to likewise be allowable over the applied reference based at least on their dependency from claim 19 for the reasons discussed above.

Dependent Claim 21

Dependent claim 21 depends indirectly from independent claim 19 and thus inherits all limitations of claim 19. Therefore, dependent claim 21 is believed allowable over the applied reference based at least on its dependency from claim 19 for the reasons presented above.

Dependent claim 20 depends from claim 19 and further recites:

receiving from said first patient, a first access key, of said plurality of access keys, that grants to said medical service provider a patient-defined level of access to the first set of medical records; and

receiving, from said second patient, a second access key, of said plurality of access keys, that grants to said medical service provider a patient-defined level of access to the second set of medical records.

Dependent claim 21 depends from claim 20 and further recites "storing, by said key organization system, the first and second access keys in the centralized key repository." Thus, claim 21 recites storing in a centralized key repository the first and second access keys that are received in the "receiving" operations of claim 20. *Soong* does not teach storing such access

keys that grant to a medical service provider a patient-defined level of access to medical records in a centralized key repository. Instead, in *Soong* the patient's password is sent from the patient to the medical service provider(s) and any other users (e.g., family members), who then individually store the password and directly input the password when accessing the patient's medical records.

Thus, claim 21 is not anticipated by *Soong*, and therefore the rejection of claim 21 should be overturned for this further reason.

Dependent Claim 22

Dependent claim 22 depends from independent claim 19 and thus inherits all limitations of claim 19. Therefore, dependent claim 22 is believed allowable over the applied reference based at least on its dependency from claim 19 for the reasons presented above.

Dependent claim 22 further recites "accessing, by said key organization system, the first set of medical records using the first access key." Thus, claim 22 recites that a key organization system uses a first access key to access the first set of medical records. *Soong* does not teach this limitation. Instead, in *Soong* a medical service provider directly inputs a patient's password in order to access the patient's medical records.

Thus, claim 22 is not anticipated by *Soong*, and therefore the rejection of claim 22 should be overturned for this further reason.

Dependent Claim 23

Dependent claim 23 depends from independent claim 19 and thus inherits all limitations of claim 19. Therefore, dependent claim 23 is believed allowable over the applied reference based at least on its dependency from claim 19 for the reasons presented above.

Dependent claim 23 further recites "accessing, by said key organization system, the second set of medical records using the second access key." Thus, claim 22 recites that a key organization system uses a second access key to access the second set of medical records. *Soong*

does not teach this limitation. Instead, in *Soong* a medical service provider directly inputs a patient's password in order to access the patient's medical records.

Thus, claim 23 is not anticipated by *Soong*, and therefore the rejection of claim 23 should be overturned for this further reason.

Independent Claim 28 and Dependent Claims 29-33

Independent claim 28 recites:

A key organization system comprising:
a server system including a computer processor and associated memory,
the server system having a centralized key repository and a centralized medical record repository;
wherein the server system is configured to:
store a first set of medical records and a second set of medical records on the centralized medical record repository;
receive a first access key associated with a medical service provider that grants to said medical service provider a patient-defined level of access to the first set of medical records;
receive a second access key associated with said medical service provider that grants to said medical service provider a patient-defined level of access to the second set of medical records; and
store the first access key and the second access key on the centralized key repository; and
wherein the key organization system is configured to, responsive to receipt of a request from the medical service provider to access one of said first and second set of medical records, retrieve a determined one of the first and second access keys from the centralized key repository and use the retrieved access key to control access by said medical service provider to said requested set of medical records. (Emphasis added).

Soong fails to teach at least the above-emphasized limitations of claim 28 as discussed further below.

First, *Soong* does not teach a server system that is configured to receive first and second access keys that are associated with a medical service provider, which grant the medical service provider access to first and second sets of medical records, respectively, as recited by claim 28. As discussed above with independent claims 1, 12, and 19, *Soong* does not disclose any

association of access keys with medical service providers. In *Soong*, the password for a patient's medical records may be distributed by the patient to any other user (e.g., physician, family member, etc.), and any user possessing the password is able to access the patient's medical records. Thus, *Soong* fails to teach this limitation of claim 28.

Further, *Soong* fails to teach a key organization system that is configured to, "responsive to receipt of a request from the medical service provider to access one of said first and second set of medical records, retrieve a determined one of the first and second access keys from the centralized key repository and use the retrieved access key to control access by said medical service provider to said requested set of medical records" (emphasis added). Rather than a key organization system retrieving and using an access key from a centralized key repository, *Soong* requires a requesting user (e.g., physician) to input a password that is used for controlling access to the medical records.

In addition, *Soong* does not teach a key organization system that controls access by the medical service provider to the requested set of medical records using the access key retrieved by the key organization system. Instead, *Soong* requires a requesting user (e.g., physician) to input a password that is used for controlling access to the medical records. No key organization system is proposed by *Soong* for retrieving an access key that is associated with a medical service provider and using that retrieved access key for controlling access to medical records.

Accordingly, *Soong* fails to teach all limitations of claim 28, and thus fails to anticipate claim 28 under 35 U.S.C. §102. Therefore, the rejection of claim 28 should be overturned for the above reasons. Dependent claims 29-33 each depend either directly or indirectly from independent claim 28 and are thus believed to likewise be allowable over the applied reference based at least on their dependency from claim 28 for the reasons discussed above.

Independent Claim 34

Independent claim 34 recites:

A computer program product residing on a computer readable medium having a plurality of instructions stored thereon which, when executed by the processor, cause a key organization system to:

receive, at said key organization system, a first access key that grants to a first medical service provider a first patient-defined level of access to a first set of medical records of a corresponding patient;

receive, at said key organization system, a second access key that grants to a second medical service provider a second patient-defined level of access to said first set of medical records of said corresponding patient;

store the first and second access keys in a centralized key repository; and responsive to a request received from one of said first and second medical service providers to access said first set of medical records, retrieve from said centralized key repository a determined one of said access keys that is associated with said requesting medical service provider, and using the retrieved access key to grant to the requesting medical service provider the corresponding patient-defined level of access to said first set of medical records. (Emphasis added).

Soong fails to teach at least the above-emphasized limitations as discussed further below.

First, *Soong* fails to teach receiving at a key organization system a first access key that grants to a first medical service provider a first patient-defined level of access to a first set of medical records. Similarly, *Soong* does not teach receiving at the key organization system a second access key that grants to a second medical service provider a second patient-defined level of access to the first set of medical records. As discussed above, instead of receiving access keys at a key organization system that grant access rights to a corresponding medical service provider, *Soong* proposes use of passwords in which a patient distributes the passwords to any person (e.g., physician, family member, etc.) who may then directly use the received password for accessing the patient's medical records.

Further, *Soong* does not teach a key organization system that, responsive to a request received from one of the first and second medical service providers to access the first set of medical records, retrieve from said centralized key repository a determined one of said access keys that is associated with said requesting medical service provider, and using the retrieved

access key to grant to the requesting medical service provider the corresponding patient-defined level of access to said first set of medical records” (emphasis added). Rather than a key organization system retrieving and using an access key from a centralized key repository, *Soong* requires a requesting user (e.g., physician) to input a password that is used for controlling access to the medical records.

In addition, *Soong* does not teach a key organization system that controls access by the medical service provider to the requested set of medical records using the access key retrieved by the key organization system. Instead, *Soong* requires a requesting user (e.g., physician) to input a password that is used for controlling access to the medical records. No key organization system is proposed by *Soong* for retrieving an access key that is associated with a medical service provider and using that retrieved access key for controlling access to medical records.

Accordingly, *Soong* fails to teach all limitations of claim 34, and thus fails to anticipate claim 34 under 35 U.S.C. §102. Therefore, the rejection of claim 34 should be overturned for the above reasons.

Independent Claim 35

Claim 35 recites:

A computer program product residing on a computer readable medium having a plurality of instructions stored thereon which, when executed by the processor, cause a key organization system to:

receive, from a patient at a key organization system, a first access key associated with a first medical service provider that grants to said first medical service provider a first patient-defined level of access to a first set of medical records;

receive, from said patient at said key organization system, a second access key associated with a second medical service provider that grants to said second medical service provider a second patient-defined level of access to said first set of medical records;

store the first and second access keys in a centralized key repository;
receive a request from said first medical service provider to access said first set of medical records; and

retrieve, responsive to said request, said first access key from said centralized key repository to provide said first medical service provider with access to said first set of medical records wherein input of said first access key from said first medical service provider is not required by said key organization system. (Emphasis added).

Soong fails to teach at least the above-emphasized limitations as discussed further below.

First, *Soong* fails to teach receiving from a patient at a key organization system a first access key associated with a first medical service provider that grants to the first medical service provider a first patient-defined level of access to a first set of medical records. Similarly, *Soong* does not teach receiving from a patient at the key organization system a second access key associated with a second medical service provider that grants to the second medical service provider a second patient-defined level of access to the first set of medical records.

As discussed above, instead of receiving an access key from a patient at a key organization system which is associated with a medical service provider to grant access rights to such medical service provider, *Soong* proposes use of passwords in which a patient distributes the passwords to any person (e.g., physician, family member, etc.) who may then directly use the received password for accessing the patient's medical records. The passwords in *Soong* are

associated with a given patient's medical records, but are not associated in any way with a medical service provider – instead, any person (e.g., medical service provider or other person) who directly possesses the password may use the password to access the patient's medical records in *Soong*.

Further, *Soong* does not teach a key organization system that, responsive to a request received from the first medical service provider to access the first set of medical records, “retrieve ... said first access key from said centralized key repository to provide said first medical service provider with access to said first set of medical records wherein input of said first access key from said first medical service provider is not required by said key organization system” (emphasis added). Instead, *Soong* requires a medical service provider to input the password received from a patient in order to access the patient's medical records. *Soong* does not teach any key organization system that retrieves an access key from a centralized repository and uses the retrieved access key to grant the medical service provider requested access to medical records, but instead requires a medical service provider to directly input a password received from a patient in order to access the patient's medical records.

Accordingly, *Soong* fails to teach all limitations of claim 35, and thus fails to anticipate claim 35 under 35 U.S.C. §102. Therefore, the rejection of claim 35 should be overturned for the above reasons.

Independent Claim 36

Independent claim 36 recites:

A computer program product residing on a computer readable medium that is communicatively coupled to a server having a plurality of instructions stored thereon which, when executed by a processor of the server cause a key organization system to:

store a plurality of patient-associated medical records on a centralized medical record repository, wherein said plurality of patient-associated medical records comprise at least of a first set of medical records associated with a first patient and a second set of medical records associated with a second patient;

store a plurality of provider-associated access keys on a centralized key repository, wherein said plurality of provider-associated access keys comprise a first access key that grants a patient-defined level of access to the first set of medical records and a second access key that grants a patient-defined level of access to the second set of medical records;

responsive to a received request from a provider to access one of said first and second sets of medical records, retrieve from said centralized key repository a respective one of said first and second access keys that grants the requesting provider a patient-defined level of access to the requested one of said first and second sets of medical records; and

use said retrieved access key to grant said requesting provider the corresponding patient-defined level of access to the requested one of said first and second sets of medical records. (Emphasis added).

Soong fails to teach at least the above-emphasized limitations of claim 36 as discussed below.

First, as discussed above, *Soong* does not teach provider-associated access keys that are stored on a centralized key repository. The passwords in *Soong* are not associated with a provider, but may instead be directly used by any person who possesses the passwords in order to access medical records.

Further, *Soong* does not teach a key organization system that, “responsive to a received request from a provider to access one of said first and second sets of medical records, retrieve from said centralized key repository a respective one of said first and second access keys that grants the requesting provider a patient-defined level of access to the requested one of said first

and second sets of medical records” (emphasis added). In *Soong*, a user (e.g., provider) directly input a corresponding password received from a patient when requesting to access that patient’s medical records. *Soong* does not teach retrieving an access key from a centralized repository responsive to a received request to access medical records, in the manner recited by claim 36.

Finally, *Soong* does not teach a key organization system that uses “said retrieved access key to grant said requesting provider the corresponding patient-defined level of access to the requested one of said first and second sets of medical records”. Again, *Soong* does not teach a key organization system that retrieves an access key responsive to an access request, and thus it also does not teach using any such retrieved access key in the manner recited by claim 36. Instead, *Soong* discloses uses a password (received by a physician from a patient) that is directly input by the physician when the physician is requesting access to the patient’s medical records.

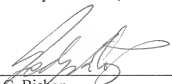
Accordingly, *Soong* fails to teach all limitations of claim 35, and thus fails to anticipate claim 35 under 35 U.S.C. §102. Therefore, the rejection of claim 35 should be overturned for the above reasons.

Conclusion

In view of the above, Appellant requests that the board overturn the outstanding rejections of claims 1-5 and 7-40. Attached hereto are a Claims Appendix, Evidence Appendix, and Related Proceedings Appendix. As noted in the attached Evidence Appendix, no evidence is submitted herewith. Also, as noted in Section II of this appeal brief, there are no related appeals are identified in Section II above, and thus as noted by the Related Proceedings Appendix, no decisions in any such related proceedings are provided.

Dated: November 2, 2009

Respectfully submitted,

By 

Jody C. Bishop
Registration No.: 44,034
FULBRIGHT & JAWORSKI L.L.P.
2200 Ross Avenue, Suite 2800
Dallas, Texas 75201-2784
(214) 855-8007
(214) 855-8200 (Fax)
Attorney for Applicant

VIII. CLAIMS APPENDIX

Claims Involved in the Appeal of Application Serial No. 10/726,423

1. A key organization method comprising:
receiving, by a key organization system operable on a computer processor, a first access key that grants, to a medical service provider, a patient-defined level of access to a first set of medical records;
receiving, by said key organization system, a second access key that grants, to said medical service provider, a patient-defined level of access to a second set of medical records;
storing the first and second access keys in a centralized key repository that is communicatively accessible by said key organization system; and
associating, by said key organization system, said first and second access keys with said medical service provider.
2. The method of claim 1 wherein the first access key is generated by a first patient, and the first set of medical records concern the first patient.
3. The method of claim 1 wherein the second access key is generated by a second patient, and the second set of medical records concern the second patient.
4. The method of claim 1 further comprising controlling, by said key organization system, said medical service provider's access to the first set of medical records by allowing said medical service provider to select, from a list of patients for whom access keys are associated with said medical service provider, a corresponding patient to whom the first set of medical records pertains.
5. The method of claim 4 further comprising controlling, by said key organization system, said medical service provider's access to the second set of medical records by allowing said medical service provider to select, from said list of patients, a corresponding patient to whom the second set of medical records pertains.

6. (Canceled)

7. The method of claim 1 further comprising storing the first and second medical records on a centralized medical record repository.

8. The method of claim 7 wherein the centralized medical record repository and centralized key repository reside on and are executed by a remote server connected to a distributed computing network.

9. The method of claim 8 wherein:
the remote server is a web server; and
the distributed computing network is the Internet.

10. The method of claim 1 wherein the first set of medical records is a multi-portion medical record and the first access key provides access to one or more portions of the first set of medical records.

11. The method of claim 1 wherein the second set of medical records is a multi-portion medical record and the second access key provides access to one or more portions of the second set of medical records.

12. A key distribution method comprising:

receiving, by the key organization system from a first patient using a client computer, a first access key that grants, to a medical service provider, a patient-defined level of access to a first set of medical records;

receiving, by the key organization system from a second patient using a second client computer, a second access key that grants, to said medical service provider, a patient-defined level of access to a second set of medical records; and

associating, by said key organization system, said first and second access keys to said medical service provider;

storing, by said key organization system, the first and second access keys and said association in a centralized key repository; and

receiving, by said key organization system, a request from said medical service provider to access said first or second set of medical records and, responsive to said request, controlling access to said requested set of medical records using said first or second access key, wherein input of said first or second access key from said medical service provider is not required by said key organization system.

13. The method of claim 12 further comprising controlling, by said key organization system, said medical service provider's access to the first set of medical records by receiving input from said medical service provider for selecting, from a list of patients for whom access keys are associated with said medical service provider, a corresponding patient to whom the first set of medical records pertains.

14. The method of claim 12 further comprising controlling, by said key organization system, said medical service provider's access to the second set of medical records by receiving input from said medical service provider for selecting, from a list of patients for whom access keys are associated with said medical service provider, a corresponding patient to whom the second set of medical records pertains.

15. The method of claim 12 further comprising storing the first and second medical records on a centralized medical record repository.

16. The method of claim 15 wherein the centralized medical record repository and centralized key repository reside on and are accessible through said key organization system connected to a distributed computing network.

17. The method of claim 12 wherein the first set of medical records is a multi-portion medical record and the first access key provides access to one or more portions of the first set of medical records.

18. The method of claim 12 wherein the second set of medical records is a multi-portion medical record and the second access key provides access to one or more portions of the second set of medical records.

19. A key organization method comprising:
maintaining, on a remote server, a centralized key repository and a centralized medical record repository;
storing a plurality of patient medical records on the centralized medical record repository, wherein said plurality of patient medical records comprise at least of a first set of medical records containing medical information pertaining a first patient and a second set of medical records containing medical information pertaining a second patient;
storing, in said centralized key repository, a plurality of access keys that each grant patient-defined access rights to a corresponding patient's set of medical records; and
responsive to a request received from a medical service provider to access one of said sets of medical records, retrieving, by a key organization system, from said centralized key repository a determined one of said access keys that is associated with said medical service provider and which corresponds to said requested set of medical records, and controlling, by said key organization system, access by said medical service provider to said requested set of medical records using the retrieved access key.

20. The method of claim 19 further comprising:
receiving from said first patient, a first access key, of said plurality of access keys, that grants to said medical service provider a patient-defined level of access to the first set of medical records; and

receiving, from said second patient, a second access key, of said plurality of access keys, that grants to said medical service provider a patient-defined level of access to the second set of medical records.

21. The method of claim 20 further comprising storing, by said key organization system, the first and second access keys in the centralized key repository.

22. The method of claim 19 further comprising accessing, by said key organization system, the first set of medical records using the first access key.

23. The method of claim 19 further comprising accessing, by said key organization system, the second set of medical records using the second access key.

24. The method of claim 19 wherein the centralized medical record repository and centralized key repository reside on a remote server connected to a distributed computing network and are communicatively coupled to said key organization system.

25. The method of claim 24 wherein:
the remote server is a web server; and
the distributed computing network is the Internet.

26. The method of claim 19 wherein the first set of medical records is a multi-portion medical record and the first access key provides access to one or more portions of the first set of medical records.

27. The method of claim 19 wherein the second set of medical records is a multi-portion medical record and the second access key provides access to one or more portions of the second set of medical records.

28. A key organization system comprising:
a server system including a computer processor and associated memory, the server system having a centralized key repository and a centralized medical record repository;
wherein the server system is configured to:
store a first set of medical records and a second set of medical records on the centralized medical record repository;

receive a first access key associated with a medical service provider that grants to said medical service provider a patient-defined level of access to the first set of medical records;

receive a second access key associated with said medical service provider that grants to said medical service provider a patient-defined level of access to the second set of medical records; and

store the first access key and the second access key on the centralized key repository; and
wherein the key organization system is configured to, responsive to receipt of a request from the medical service provider to access one of said first and second set of medical records, retrieve a determined one of the first and second access keys from the centralized key repository and use the retrieved access key to control access by said medical service provider to said requested set of medical records.

29. The system of claim 28 further comprising a client system including a computer processor and associated memory, the client system being configured to:

communicate said request from said medical service provider to said key organization system via a communication network.

30. The system of claim 29 wherein the server system and the client system are coupled via a distributed computing network.

31. The system of claim 30 wherein the distributed computing network is the Internet.

32. The system of claim 28 wherein the first set of medical records is a multi-portion medical record and the first access key provides access to one or more portions of the first set of medical records.

33. The method of claim 28 wherein the second set of medical records is a multi-portion medical record and the second access key provides access to one or more portions of the second set of medical records.

34. A computer program product residing on a computer readable medium having a plurality of instructions stored thereon which, when executed by the processor, cause a key organization system to:

receive, at said key organization system, a first access key that grants to a first medical service provider a first patient-defined level of access to a first set of medical records of a corresponding patient;

receive, at said key organization system, a second access key that grants to a second medical service provider a second patient-defined level of access to said first set of medical records of said corresponding patient;

store the first and second access keys in a centralized key repository; and

responsive to a request received from one of said first and second medical service providers to access said first set of medical records, retrieve from said centralized key repository a determined one of said access keys that is associated with said requesting medical service provider, and using the retrieved access key to grant to the requesting medical service provider the corresponding patient-defined level of access to said first set of medical records.

35. A computer program product residing on a computer readable medium having a plurality of instructions stored thereon which, when executed by the processor, cause a key organization system to:

receive, from a patient at a key organization system, a first access key associated with a first medical service provider that grants to said first medical service provider a first patient-defined level of access to a first set of medical records;

receive, from said patient at said key organization system, a second access key associated with a second medical service provider that grants to said second medical service provider a second patient-defined level of access to said first set of medical records;

store the first and second access keys in a centralized key repository;

receive a request from said first medical service provider to access said first set of medical records; and

retrieve, responsive to said request, said first access key from said centralized key repository to provide said first medical service provider with access to said first set of medical records wherein input of said first access key from said first medical service provider is not required by said key organization system.

36. A computer program product residing on a computer readable medium that is communicatively coupled to a server having a plurality of instructions stored thereon which, when executed by a processor of the server cause a key organization system to:

store a plurality of patient-associated medical records on a centralized medical record repository, wherein said plurality of patient-associated medical records comprise at least of a first set of medical records associated with a first patient and a second set of medical records associated with a second patient;

store a plurality of provider-associated access keys on a centralized key repository, wherein said plurality of provider-associated access keys comprise a first access key that grants a patient-defined level of access to the first set of medical records and a second access key that grants a patient-defined level of access to the second set of medical records;

responsive to a received request from a provider to access one of said first and second sets of medical records, retrieve from said centralized key repository a respective one of said first and second access keys that grants the requesting provider a patient-defined level of access to the requested one of said first and second sets of medical records; and

use said retrieved access key to grant said requesting provider the corresponding patient-defined level of access to the requested one of said first and second sets of medical records.

37. The method of claim 1 further comprising:

granting said medical service provider secure access to said key organization system, wherein said access allows said medical service provider to select a patient from a group of patients associated with said medical service provider.

38. The method of claim 37 wherein said secure access is granted after said medical service provider passes a security test issued by said key organization system.

39. The method of claim 37 further comprising:

receiving, by said key organization system, said selection, wherein said selection is a request to access said first set of medical records;

retrieving from said centralized key repository, by said key organization system in response to said selection, said first access key; and

using, by said key organization system, said first access key to control said medical services provider's access to said first set of medical records.

40. The method of claim 4 wherein accessing the first set of medical records does not require said medical service provider to pass a second security test.

IX. EVIDENCE APPENDIX

No evidence pursuant to §§ 1.130, 1.131, or 1.132 or entered by or relied upon by the examiner is being submitted.

X. RELATED PROCEEDINGS APPENDIX

There are no other appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.